

1 DAVID L. ANDERSON (CABN 149604)  
United States Attorney

2 BARBARA J. VALLIERE (DCBN 439357)  
3 Chief, Criminal Division

4 ROBERT S. LEACH (CABN 196191)  
JONAS LERMAN (CABN 274733)  
5 Assistant United States Attorneys

6 1301 Clay Street, Suite 340S  
Oakland, California 94612  
7 Telephone: (510) 637-3918  
8 Fax: (510) 637-3724  
Email: robert.leach@usdoj.gov

9 Attorneys for United States of America

10 UNITED STATES DISTRICT COURT  
11 NORTHERN DISTRICT OF CALIFORNIA  
12 OAKLAND DIVISION

13 IN THE MATTER OF THE SEARCH OF A )  
14 RESIDENCE IN OAKLAND, CALIFORNIA )

No. 4-19-70053 KAW

15 ) UNITED STATES' REQUEST FOR REVIEW  
16 ) OF THE DUTY MAGISTRATE JUDGE'S  
17 ) DENIAL OF A SEARCH WARRANT  
18 ) APPLICATION

Date: January 30, 2019

Time: 10:30 a.m.

Duty Judge: The Honorable James Donato

FILED  
AUG 16 2019  
CLERK SUSAN Y. SOONG  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

5-19-71283 VKD  
SEALED BY ORDER  
OF COURT

**TABLE OF CONTENTS**

1		
2	INTRODUCTION .....	1
3	BACKGROUND .....	1
4	I. Background Regarding Biometrics*.....	1
5	II. The Government's Investigation.....	2
6	III. The Magistrate Judge's Order.....	3
7	JURISDICTION .....	4
8	ARGUMENT .....	5
9	I. The Fourth Amendment Permits the Use of Biometrics to Execute a Valid Search	
10	Warrant, But a Warrant Need Not Include Authorization to Use Biometrics. ....	6
11	II. The Fifth Amendment Permits the Government to Unlock a Device While Executing	
12	a Warranted Search by Using Biometrics. ....	8
13	CONCLUSION.....	13

**TABLE OF AUTHORITIES**

Cases

<i>Alvarez v. Smith</i> , 558 U.S. 87 (2009).....	5
<i>Bailey v. United States</i> , 568 U.S. 186 (2015) .....	6
<i>Commonwealth v. Baust</i> , 89 Va. Cir. 267, 2014 WL 10355635 (Va. Cir. Ct. Oct. 28, 2014).....	12
<i>County of Los Angeles v. Davis</i> , 440 U.S. 625 (1979).....	5
<i>Curcio v. United States</i> , 354 U.S. 118 (1957) .....	9
<i>Dalia v. United States</i> , 441 U.S. 238 (1979) .....	6
<i>Davis v. Mississippi</i> , 394 U.S. 721 (1969).....	7
<i>Doe v. United States</i> , 487 U.S. 201 (1988).....	9, 10, 11, 13
<i>Fisher v. United States</i> , 425 U.S. 391 (1976) .....	10
<i>Gilbert v. California</i> , 388 U.S. 263 (1967).....	9
<i>Gomez v. United States</i> , 490 U.S. 858 (1989) .....	4
<i>Hiibel v. Sixth Judicial Dist. Court</i> , 542 U.S. 177 (2004) .....	8
<i>In re Application for a Search Warrant</i> , 236 F. Supp. 3d 1066 (N.D. Ill. 2017) .....	11
<i>In re Search of Fair Finance</i> , 692 F.3d 424 (6th Cir. 2012) .....	5
<i>In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.</i> , 212 F. Supp. 3d 1023 (D. Kan. 2016) .....	4
<i>In re Search of [Redacted] Washington, DC</i> , 317 F. Supp. 3d 523 (D.D.C. 2018) .....	8, 12, 13
<i>In re Search Warrant Application for [Redacted Text]</i> , 279 F. Supp. 3d 800 (N.D. Ill. 2017).....	11, 12
<i>Katz v. United States</i> , 389 U.S. 347 (1967) .....	7
<i>Maryland v. King</i> , 569 U.S. 435 (2013) .....	7
<i>Michigan v. Summers</i> , 452 U.S. 692 (1981).....	6, 7
<i>Minnesota v. Diamond</i> , 905 N.W.2d 870 (2018).....	12
<i>Muehler v. Mena</i> , 544 U.S. 93 (2005) .....	6, 7
<i>N. Mariana Islands v. Bowie</i> , 243 F.3d 1109 (9th Cir. 2001) .....	9
<i>Perry v. Schwarzenegger</i> , 268 F.R.D. 344 (N.D. Cal. 2010) .....	4
<i>Phoenix Newspapers, Inc. v. U.S. Dist. Court</i> , 156 F.3d 940 (9th Cir. 1998).....	5

1	<i>Schmerber v. California</i> , 384 U.S. 757 (1966) .....	7, 9, 12
2	<i>S. Pac. Terminal Co. v. ICC</i> , 219 U.S. 498 (1911).....	5
3	<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006).....	8
4	<i>United States v. Brobst</i> , 558 F.3d 982 (9th Cir. 2009).....	8
5	<i>United States v. Brooklier</i> , 685 F.2d 1162 (9th Cir. 1982).....	5
6	<i>United States v. De Palma</i> , 414 F.2d 394 (9th Cir. 1969) .....	9
7	<i>United States v. Dionisio</i> , 410 U.S. 1 (1973).....	7, 9
8	<i>United States v. Doe</i> , 457 F.2d 895 (2d Cir. 1972).....	7
9	<i>United States v. Emmett</i> , 321 F.3d 669 (7th Cir. 2003) .....	7
10	<i>United States v. Grubbs</i> , 547 U.S. 90 (2006).....	6
11	<i>United States v. Hubbell</i> , 530 U.S. 27 (2000).....	8, 9, 10, 13
12	<i>United States v. Krupa</i> , 658 F.3d 1174 (9th Cir. 2011) .....	8
13	<i>United States v. Lacy</i> , 119 F.3d 742 ( 9th Cir. 1997) .....	8
14	<i>United States v. Raddatz</i> , 447 U.S. 667 (1980) .....	5
15	<i>United States v. Sanudo-Duarte</i> , No. CR-14-01342-002-PHX-JAT, 2016 WL 126283 (D. Ariz. Jan. 12, 2016) .....	9
16	<i>United States v. Schesso</i> , 730 F.3d 1040 (9th Cir. 2013).....	8
17	<i>United States v. Spencer</i> , 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018) .....	10
18	<i>United States v. Wade</i> , 388 U.S. 218 (1967) .....	9
19	<i>In re United States</i> , 791 F.3d 945 (9th Cir. 2015) .....	5
20	<i>Weinstein v. Bradford</i> , 423 U.S. 147 (1975).....	5
21	<i>Yezek v. Mitchell</i> , No. 05-C-3461 TEH, 2007 WL 61887 (N.D. Cal. Jan. 8, 2007).....	7

#### Statutes

24	18 U.S.C. § 875.....	2, 8
25	28 U.S.C. § 631 .....	4
26	28 U.S.C. § 636(b)(1)(A).....	4

## INTRODUCTION

On January 10, 2019, without the benefit of briefing, Magistrate Judge Kandis A. Westmore, the duty magistrate, issued a published order denying a search warrant application relating to an active law enforcement investigation. The requested search warrant would have permitted law enforcement officers, while searching a residence, to compel certain individuals there (including two identified subjects) to press a finger to certain digital devices found in the residence to unlock them. This practice, often called “use of biometrics,” has been approved by magistrates in this District, both before and after the Magistrate Judge’s ruling. It also has been approved by the majority of other courts to have considered the issue.

The Magistrate Judge’s order is wrong, and this Court should overrule it or, at a minimum, vacate it. Because applying a subject’s fingerprint to a device is not “testimonial,” compelling a person to do so does not violate the Fifth Amendment privilege against self-incrimination. Use of biometrics is no more a Fifth Amendment violation than a host of practices approved as constitutional by the Supreme Court and the Ninth Circuit, including fingerprinting, photographing a subject, obtaining a voice or handwriting exemplar, or extracting a blood sample.

The Magistrate Judge, based largely on her conclusion that use of biometrics is testimonial under the Fifth Amendment, concluded that the search warrant application also violated the Fourth Amendment. That aspect of the Magistrate Judge’s ruling also requires reversal or vacatur. Because a valid search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted, and because a valid warrant need not include all details about how agents will execute it, the proposed warrant satisfied the Fourth Amendment.

## BACKGROUND

### I. Background Regarding Biometrics

Apple, Samsung, and other companies produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple’s is called Touch ID. Apple also has a feature called Face ID, which allows certain

1 iPhones to be unlocked with the user's face. Once a user has set up the fingerprint or face sensor feature  
2 in the security settings of the device, the user can unlock the device by placing a finger or thumb on the  
3 device's fingerprint sensor. If that sensor recognizes the fingerprint or face, the device unlocks. For  
4 fingerprint features, most devices can be set up to recognize multiple prints, so that different prints, not  
5 necessarily from the same person, will unlock the device. If there is no sensor on the device, the device  
6 will not open with prints.

7       There are limits on the ability to use a fingerprint or thumbprint to unlock a device, which varies  
8 by manufacturer. For example, with Apple, the Touch ID feature only permits up to five attempts with a  
9 print before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will  
10 not substitute for the use of a passcode or password if more than 48 hours have passed since the device  
11 has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the  
12 device will require the passcode or password programmed by the user and will not allow access to the  
13 device based on a print alone. Similarly, Touch ID will not allow access if the device has been restarted  
14 or was off and has been turned on, if the device has received a remote lock command, or if five attempts  
15 to match a print have been unsuccessful. Other brands have similar restrictions.

## 16 **II. The Government's Investigation**

17       The government is investigating possible extortion, in violation of 18 U.S.C. § 875(d), involving  
18 the use of a social media platform.

19       On January 3, 2019, the government submitted an application for a warrant to search a residence  
20 in Oakland ("Subject Premises") and certain digital devices found at the Subject Premises for evidence,  
21 instrumentalities, and contraband relating to the offense. *See* ECF No. 1 at 1.<sup>1</sup> The government's  
22 application sought permission to compel certain individuals to unlock a device subject to seizure using  
23 the device's biometric features. *See* Application for a Search Warrant ¶ 17. Specifically, in the  
24 proposed warrant, the government requested authority for "law enforcement personnel . . . to (1) press or  
25 swipe the fingers (including thumbs) of any individual, who is found at the [S]ubject [P]remises and  
26

27 <sup>1</sup> The application and the proposed warrant were filed under seal under this case number. Because  
28 the investigation is ongoing and not fully known to all of the subjects of the investigation, the  
government respectfully requests the Court continue to maintain them under seal. The government will  
lodge courtesy copies of the sealed filings with Chambers.



1 reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the  
2 device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those  
3 same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the  
4 premises in front of the face of those same individuals and activate the iris recognition feature, for the  
5 purpose of attempting to unlock the device(s) in order to search the contents as authorized by this search  
6 warrant.” See [Proposed] Search and Seizure Warrant at Attachment B, ¶ 7.

### 7 **III. The Magistrate Judge’s Order**

8 On January 10, 2019, without the benefit of briefing from the government, the Court issued an  
9 unsealed order denying the application. ECF No. 1. The Magistrate Judge found “there are sufficient  
10 facts in the affidavit to believe that evidence of the crime will be found at the Subject Premises, so the  
11 Government has probable cause to conduct a lawful search, so long as it comports with the Fourth  
12 Amendment.” *Id.* at 2. The Magistrate Judge further found probable cause to “seize those digital  
13 devices that law enforcement reasonably believes are owned and/or possessed by the two suspects  
14 named in the affidavit.” *Id.* at 9. The Magistrate Judge nonetheless denied the application because it  
15 sought permission to compel certain individuals to unlock a device subject to seizure using the device’s  
16 biometric features. The Magistrate Judge held, categorically, that “[t]he Government may not compel or  
17 otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock  
18 electronic devices” on the ground that it would run afoul of the Fifth Amendment right against self-  
19 incrimination. *Id.* at 9. The Court further held that the proposed warrant would violate the Fourth  
20 Amendment. *Id.* at 3.

21 The Magistrate Judge’s unsealed order gave notice to those in Oakland (and elsewhere) that the  
22 government was investigating use of a particular social media to commit extortion through particular  
23 means and was focused on a residence in Oakland. Within a week of the order, numerous news outlets  
24 published stories about it.<sup>2</sup>

25  
26 <sup>2</sup> E.g., Cyrus Farivar, *Feds forcing mass fingerprint unlocks is an “abuse of power,” judge rules*,  
27 ARS TECHNICA, Jan. 14, 2019, <https://arstechnica.com/tech-policy/2019/01/feds-forcing-mass-fingerprint-unlocks-is-an-abuse-of-power-judge-rules/>; Thomas Brewster, *Feds Can’t Force You to Unlock Your iPhone with Finger or Face, Judge Rules*, FORBES, Jan. 14, 2019,  
28 <https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/>; Rhett Jones, *Cops Can’t Force People to Unlock Their Phones with Biometrics, Court Rules*, GIZMODO, Jan. 14, 2019, <https://gizmodo.com/cops-cant-force-people-to-u.s.-request-for-review-of-the-duty-magistrate-judge-s-denial-of-search-warrant>

1 On January 10, 2019, the day the Magistrate Judge's order was issued, in part to minimize the  
2 risk that evidence would be destroyed or moved, the government submitted a new search warrant  
3 application that, at the Magistrate Judge's request, omitted any reference to use of biometrics and sought  
4 authority to search only devices owned or controlled by two named individuals. The Magistrate Judge  
5 issued the new warrant on January 11, 2019. That new warrant has been executed.

### 6 JURISDICTION

7 Under the Federal Magistrates Act, 28 U.S.C. § 631, *et seq.*, magistrate judges have the authority  
8 to decide pretrial, non-dispositive matters. 28 U.S.C. § 636(b)(1)(A). Included within this pretrial  
9 authority is the issuance of search warrants. *See Gomez v. United States*, 490 U.S. 858, 868 n.16 (1989).  
10 Pursuant to the Federal Magistrates Act, "[a] judge of the court may reconsider any [non-dispositive]  
11 pretrial matter . . . where it has been shown that the magistrate judge's order is clearly erroneous or  
12 contrary to law." 28 U.S.C. § 636(b)(1)(A); *see In re Search of Info. Associated with Email Addresses*  
13 *Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023, 1029 (D. Kan. 2016).  
14 "The magistrate's legal conclusions are reviewed de novo to determine whether they are contrary to  
15 law." *Perry v. Schwarzenegger*, 268 F.R.D. 344, 348 (N.D. Cal. 2010).

16 Notwithstanding the execution of the new warrant, a live controversy exists here. The  
17 Magistrate Judge's order involves a practice that directly affects the government, and the Magistrate  
18 Judge has made clear that she will not sign any search warrants that provide for use of biometrics to  
19 unlock electronic devices, as she believes use of biometrics violates both the Fourth and Fifth  
20 Amendments. Indeed, in the days immediately after she issued her order, she refused to sign other  
21 search warrant applications on the same grounds. This dispute is not moot merely because the

22  
23 unlock-their-phones-with-biom-1831743969; Orin Kerr, *Search Warrants and Compelled Biometric*  
24 *Access to Phones*, VOLOKH CONSPIRACY, Jan. 15, 2019, [https://reason.com/volokh/2019/01/15/search-](https://reason.com/volokh/2019/01/15/search-warrants-and-compelled-biometric)  
25 *warrants-and-compelled-biometric*; Nicole Darrah, *Authorities can't force people to unlock technology*  
26 *with biometric features*, US judge rules, FOX NEWS, Jan. 15, 2019, [https://www.foxnews.com/tech/us-](https://www.foxnews.com/tech/us-authorities-cant-force-people-to-unlock-technology-with-fingerprint-facial-recognition-judge-rules)  
27 *authorities-cant-force-people-to-unlock-technology-with-fingerprint-facial-recognition-judge-rules*;  
28 Marrian Zhou, *Police can't force you to unlock phone with Face ID or fingerprint*, judge rules, CNET,  
Jan. 15, 2019, [https://www.cnet.com/news/police-cant-force-you-to-unlock-phone-with-face-id-or-](https://www.cnet.com/news/police-cant-force-you-to-unlock-phone-with-face-id-or-fingerprint-judge-rules/)  
fingerprint-judge-rules/; Mariella Moon, *US judge rules that feds can't force fingerprint or face phone*  
unlocks, ENGADGET, Jan. 15, 2019, [https://www.engadget.com/2019/01/15/judge-biometrics-unlocking-](https://www.engadget.com/2019/01/15/judge-biometrics-unlocking-rule/)  
rule/; Ian Lopez, *A California Judge May Have Changed the Conversation Around Biometrics Privacy*  
Rights, RECORDER, Jan. 17, 2019, [https://www.law.com/therecorder/2019/01/17/a-california-judge-may-](https://www.law.com/therecorder/2019/01/17/a-california-judge-may-have-changed-the-conversation-around-biometrics-privacy-rights/)  
have-changed-the-conversation-around-biometrics-privacy-rights/.



1 government in this case resubmitted a new warrant application to the Magistrate Judge, at her request,  
2 after she refused to sign the original warrant. The government's action was purely one of necessity,  
3 resulting from the time sensitivity of an active investigation and from the Magistrate Judge's decision to  
4 publish her order publicly, which potentially put targets on notice of the government's investigation.

5 In general, a case is moot when the issues presented are no longer live or the parties lack a  
6 legally cognizable interest in the outcome. *County of Los Angeles v. Davis*, 440 U.S. 625, 631 (1979).  
7 The Supreme Court has recognized several well-established exceptions to the mootness doctrine,  
8 including if a dispute is "capable of repetition, yet evading review." *S. Pac. Terminal Co. v. ICC*, 219  
9 U.S. 498, 515 (1911). A dispute is capable of repetition if "there [is] a reasonable expectation that the  
10 same complaining party would be subjected to the same action again," and it is likely to evade review if  
11 "the challenged action was in its duration too short to be fully litigated prior to its cessation or  
12 expiration." *Weinstein v. Bradford*, 423 U.S. 147, 149 (1975) (per curiam). That exception applies here.  
13 See, e.g., *In re Search of Fair Finance*, 692 F.3d 424, 428–29 (6th Cir. 2012); *Phoenix Newspapers, Inc.*  
14 *v. U.S. Dist. Court*, 156 F.3d 940, 946 (9th Cir. 1998); *United States v. Brooklier*, 685 F.2d 1162, 1165  
15 (9th Cir. 1982).

16 Even if this matter were moot and no exception applied, this Court would have authority to  
17 vacate the Magistrate Judge's order, if not to reverse it. See *Alvarez v. Smith*, 558 U.S. 87, 94–96  
18 (2009); see also *United States v. Raddatz*, 447 U.S. 667, 681 (1980) ("Congress made clear that . . . the  
19 magistrate acts subsidiary and only in aid of the district court. . . . [T]he entire process takes place under  
20 the district court's total control and jurisdiction."). Given the important interests at stake, this Court  
21 should "offer guidance to" the Magistrate Judge and clarity to the government. See *In re United States*,  
22 791 F.3d 945, 960–61 (9th Cir. 2015).

### 23 ARGUMENT

24 Compelling a person to provide a fingerprint or thumbprint as part of a search warrant, or  
25 holding a device in front of that person's face, violates neither the Fourth nor the Fifth Amendment.

26 ///

27 ///

28 ///

1 **I. The Fourth Amendment Permits the Use of Biometrics to Execute a Valid Search Warrant,**  
2 **But a Warrant Need Not Include Authorization to Use Biometrics.**

3 The United States sought permission in its search warrant application to use individuals' hand  
4 digits and faces for the purpose of unlocking devices covered by the search warrant through the devices'  
5 biometric features, where those individuals were present at the execution of the search, the seizure  
6 occurred at the execution of the search, and where there was reasonable suspicion to believe the  
7 individuals used the device. The United States included this request not because it is required under the  
8 Fourth Amendment but because the Supreme Court has indicated that, while not required, making  
9 explicit to an authorizing court the means the government anticipates it will take to execute a search  
10 warrant is "preferable." *Dalia v. United States*, 441 U.S. 238, 258–59 & n.22 (1979) (internal quotation  
11 marks and citation omitted).

12 *Dalia* and *United States v. Grubbs*, 547 U.S. 90, 98 (2006), clearly explain that under the Fourth  
13 Amendment, search warrants need not specify the precise manner in which they are to be executed.  
14 Therefore, the United States need not specify how it intends to unlock electronic devices that a search  
15 warrant authorizes it to seize and search. The manner used by officers to execute a warrant "is subject to  
16 later judicial review as to its reasonableness." *Dalia*, 441 U.S. at 258.

17 Nor does the use of biometric data to preserve evidence covered by a search warrant require  
18 separate warrant authorization. *Dalia* also recognized that "in executing a warrant the police may find it  
19 necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."  
20 *Dalia*, 441 U.S. at 257.

21 Moreover, there is no additional seizure of the persons beyond what is already authorized by a  
22 warrant. A valid premises search warrant implicitly carries with it the limited authority to briefly detain  
23 the occupants on, or in the immediate vicinity of, the premises while the search is being conducted.  
24 *Michigan v. Summers*, 452 U.S. 692, 705 (1981). The authority to detain carries with it the authority to  
25 "use reasonable force to effectuate detention." *Muehler v. Mena*, 544 U.S. 93, 98–99 (2005). This  
26 detention prevents flight in the event that incriminating evidence is found, minimizes the risk of harm to  
27 the officers, and facilitates orderly completion of the search. *Bailey v. United States*, 568 U.S. 186, 194  
28

1 (2015); *Muehler*, 544 U.S. at 98 (“An officer’s authority to detain incident to a search is categorical . . .  
2 .”).

3       The government’s use of biometric data to unlock devices that may otherwise be unlockable  
4 furthers both the avoidance of destruction of evidence and the orderly execution of a valid search  
5 warrant. Moreover, the slight movement of a subject’s hands to take fingerprints or use a Face ID or  
6 similar technologies does not constitute a greater intrusion than the ability to direct a subject to a  
7 particular area or to handcuff a subject for the duration of the search; it is a reasonable use of force to  
8 effectuate the purposes of a limited detention set forth in *Summers*. See *Muehler*, 544 U.S. at 98–99.  
9 This practice stands in stark contrast to *Schmerber v. California*, where the Supreme Court held that  
10 although there was probable cause to arrest the defendant for driving an automobile while under the  
11 influence of intoxicating liquor, and the officer was therefore entitled to search him incident to arrest  
12 without a warrant, this did not authorize the officer to take a blood sample from the defendant. 384 U.S.  
13 757, 771 (1966). The Supreme Court held that the blood draw involved an “intrusion[] beyond the  
14 body’s surface” and implicated enhanced “interests in human dignity and privacy.” *Id.* at 769–70.

15       Further, the Fourth Amendment does not protect what a person knowingly exposes to the public.  
16 *Katz v. United States*, 389 U.S. 347, 351 (1967); *United States v. Dionisio*, 410 U.S. 1, 14 (1973). And  
17 the Supreme Court has long held that “fingerprinting itself ‘involves none of the probing into an  
18 individual’s private life and thoughts that marks an interrogation or search.’” *Dionisio*, 410 U.S. at 15  
19 (quoting *Davis v. Mississippi*, 394 U.S. 721, 727 (1969)). It is also “clear that a person has no  
20 expectation of privacy in a photograph of his face.” *United States v. Emmett*, 321 F.3d 669, 672 (7th  
21 Cir. 2003) (cited by *Yezek v. Mitchell*, No. 05-C-3461 TEH, 2007 WL 61887, at \*6 n.5 (N.D. Cal. Jan. 8,  
22 2007)); *United States v. Doe*, 457 F.2d 895, 898 (2d Cir. 1972) (same); cf. *Maryland v. King*, 569 U.S.  
23 435, 465–66 (2013) (holding that “taking and analyzing a cheek swab,” like “fingerprinting and  
24 photographing,” is “a legitimate police booking procedure that is reasonable under the Fourth  
25 Amendment”).

26       The Magistrate Judge also expressed a concern about overbreadth, stating that “[t]he  
27 Government cannot be permitted to search and seize a mobile phone or other device that is on a non-  
28 suspect’s person simply because they are present during an otherwise lawful search.” ECF No. 1 at

1 3. But the United States sought no such authorization, and the Magistrate Judge's overbreadth concerns  
2 are unfounded. Rather, the proposed warrant would have authorized seizure of "evidence, contraband,  
3 fruits, or instrumentalities of violations of 18 U.S.C. § 875" and "[c]omputers or storage media used as a  
4 means to commit [such] violations" and use of fingerprints and biometrics of individuals reasonably  
5 believed to use digital devices that the government is authorized to search. *See* [Proposed] Search and  
6 Seizure Warrant at Attachment B, ¶¶ 3, 4, & 7; *see also* Application for a Search Warrant, ¶¶ 7 &  
7 7(i). The affidavit that the United States submitted in support of the search warrant here "established  
8 both probable cause to believe that a crime had been committed and that evidence of the crime would be  
9 found at the premises to be searched, including on the Subject Devices," so the warrant is not  
10 overbroad. *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d 523, 527 & n.3 (D.D.C. 2018);  
11 *see United States v. Schesso*, 730 F.3d 1040, 1046–47 (9th Cir. 2013) (rejecting overbreadth challenge  
12 where search warrant permitted search and seizure of defendant's "entire computer system and  
13 associated digital storage devices," because "[t]he government had no way of knowing which or how  
14 many illicit files there might be or where they might be stored, or of describing the items to be seized in  
15 a more precise manner," and noting that "[w]e have repeatedly found equally broad searches  
16 constitutional on similar or less evidence" (citing *United States v. Krupa*, 658 F.3d 1174, 1178 (9th Cir.  
17 2011)); *United States v. Brobst*, 558 F.3d 982, 993–94 (9th Cir. 2009); *United States v. Lacy*, 119 F.3d  
18 742, 746 (9th Cir. 1997)); *see also United States v. Adjani*, 452 F.3d 1140, 1148–49 (9th Cir. 2006)  
19 ("Warrants which describe generic categories of items are not necessarily invalid if a more precise  
20 description of the items subject to seizure is not possible.") (internal citations omitted).

21 **II. The Fifth Amendment Permits the Government to Unlock a Device While Executing a**  
22 **Warranted Search by Using Biometrics.**

23 "[T]here is a significant difference between the use of compulsion to extort communications  
24 from a defendant and compelling a person to engage in conduct that may be incriminating." *United*  
25 *States v. Hubbell*, 530 U.S. 27, 34–35 (2000). Thus, "[t]o qualify for the Fifth Amendment privilege, a  
26 communication must be: (1) testimonial, (2) incriminating, and (3) compelled." *Hiibel v. Sixth Judicial*  
27 *Dist. Court*, 542 U.S. 177, 189 (2004). Compelling a person to provide a fingerprint, or to face a  
28

1 phone's screen, does not violate the Fifth Amendment, because even if that act is compelled *and*  
2 incriminating, it is not testimonial.

3 For decades, the Supreme Court has found numerous acts akin to the use of biometrics not to be  
4 testimonial and therefore not protected by the Fifth Amendment. "It has long been held that the  
5 compelled display of identifiable physical characteristics infringes no interest protected by the [Fifth  
6 Amendment] privilege against compulsory self-incrimination." *Dionisio*, 410 U.S. at 5–6. And the  
7 privilege "offers no protection against compulsion to submit to fingerprinting, photography, or  
8 measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to  
9 walk, or to make a particular gesture . . . [because] [n]one of these activities becomes testimonial within  
10 the scope of the privilege." *United States v. Wade*, 388 U.S. 218, 223 (1967) (quoting *Schmerber*, 384  
11 U.S. at 764); *see also Hubbell*, 530 U.S. at 35; *Gilbert v. California*, 388 U.S. 263, 266–67 (1967). The  
12 Court has explained that compelled display of physical characteristics is not testimonial because a  
13 subject is "not required to disclose any knowledge he might have, or to speak his guilt." *Doe v. United*  
14 *States*, 487 U.S. 201, 211 (1988) (internal quotation marks omitted). The subject is not required "'to  
15 disclose the contents of his own mind.'" *Id.* (quoting *Curcio v. United States*, 354 U.S. 118 (1957)).

16 The Ninth Circuit has held the same: "[r]equests by the prosecution for . . . fingerprint evidence  
17 from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination  
18 because such evidence is not testimonial in nature." *N. Mariana Islands v. Bowie*, 243 F.3d 1109, 1120  
19 n.5 (9th Cir. 2001); *see also United States v. De Palma*, 414 F.2d 394, 397 (9th Cir. 1969) ("Identifying  
20 physical characteristics are not evidence of a testimonial nature."); *United States v. Sanudo-Duarte*, No.  
21 CR-14-01342-002-PHX-JAT, 2016 WL 126283, at \*1 (D. Ariz. Jan. 12, 2016) (holding under Fourth  
22 and Fifth Amendments that defendant could be compelled to provide exemplar of his palm prints and  
23 that "palm prints are identifiable physical characteristics unprotected by the Fifth Amendment").

24 Under this well-established precedent, applying a fingerprint to an electronic device covered by a  
25 valid search warrant, or holding up a device in front of a subject's face, does not implicate the Fifth  
26 Amendment because law enforcement's action involves no compelled testimonial act by the subject. It  
27 does not require the subject to disclose the contents of his mind.  
28



1 Contrary to precedent, the Magistrate Judge conflated the Fifth Amendment privilege's three  
2 distinct requirements: compelled, incriminating, and testimonial. The Magistrate Judge concluded that  
3 use of biometrics is testimonial because "a successful finger or thumb scan confirms ownership or  
4 control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably  
5 refuted." ECF No. 1 at 6. But as the Supreme Court has made clear, the inquiry into whether an act is  
6 testimonial does not turn on whether an inference can be reasonably refuted, or indeed whether the act is  
7 incriminating.

8 That an act of unlocking a device may lead to incriminating evidence—including that the subject  
9 has control of a particular device—is irrelevant to the Fifth Amendment analysis. "If a compelled  
10 [action or] statement is not testimonial and for that reason not protected by the privilege, it cannot  
11 become so because it will lead to incriminating evidence." *Doe*, 487 U.S. at 208–09 n.6 (1988) (internal  
12 quotation marks omitted); *see also Hubbell*, 530 U.S. at 35 (recognizing that "a criminal suspect may be  
13 compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording  
14 of his voice," even if those acts may be incriminating) (citations omitted); *Fisher v. United States*, 425  
15 U.S. 391, 411 (1976) ("[A]lthough the [handwriting] exemplar may be incriminating to the accused and  
16 although he is compelled to furnish it, his Fifth Amendment privilege is not violated because nothing he  
17 has said or done is deemed to be sufficiently testimonial for purposes of the privilege.")<sup>3</sup>

18 In addition to contravening Supreme Court and Ninth Circuit precedent, the Magistrate Judge's  
19 order conflicts with decisions of lower courts—decisions that the Magistrate Judge did not acknowledge,  
20 let alone distinguish.

21 Most strikingly, while relying on the decision of a magistrate in the Northern District of Illinois,  
22 *see* ECF No. 1 at 6 (citing *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill.

23  
24 <sup>3</sup> Because law enforcement's compelled use of a subject's fingerprint or face is not a testimonial  
25 act by the subject, the Magistrate Judge had no need to analyze the "foregone conclusion" doctrine, *see*  
26 *Fisher*, 425 U.S. at 411, and the United States does not invoke that doctrine here. The United States  
27 notes, however, that the Magistrate Judge's conclusion that the foregone conclusion doctrine cannot  
28 apply to electronic devices because law enforcement cannot anticipate the "full contents" of the devices,  
*see* ECF No. 1 at 8, is squarely contrary to a recent district court opinion in this District. *See United*  
*States v. Spencer*, 2018 WL 1964588, at \*3 (N.D. Cal. Apr. 26, 2018) (holding that in order to invoke  
the foregone conclusion doctrine in the context of compelled decryption, "the government need only  
show it is a foregone conclusion that [the subject] has the ability to decrypt the devices"). The  
Magistrate Judge did not cite this opinion.

2017)), the Magistrate Judge failed to cite a subsequent contrary decision by a U.S. district judge on the same court: *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800 (N.D. Ill. 2017).

In that more recent decision, the district court reversed a magistrate judge and held that no Fifth Amendment testimonial act occurs when agents press a subject's fingers against a Touch ID sensor on an iPhone, because "the government agents will pick the fingers to be pressed on the Touch ID sensor, so there is no need to engage the thought process of any of the residents at all in effectuating the seizure," and applying the fingerprint to the sensor "is simply the seizure of a physical characteristic, and the fingerprint by itself does not communicate anything." *Id.* at 803–04. The district court distinguished the Supreme Court's *Hubbell* decision because there, "the act of producing the records inherently represented communications from the defendant," but "[n]ot so with the fingerprint seizure":

The government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without need for the person to put any thought at all into the seizure. . . . [T]he person's performance of the compelled act is not an act of communication by that person. Indeed, the person can be asleep—and thus by definition not communicating anything—when a seizure of this sort is effectuated. If anything, handwriting and voice exemplars require a person to engage more mental processes than simply providing a finger for application to the Touch ID sensor. And if anything, handwriting and voice exemplars contain more implicit admissions than a fingerprint, namely, that "I can write and this is my handwriting," or "this is my voice and this is how I pronounce this word."

*Id.* at 804 (citations omitted) (emphasis added). The court in that case also agreed with the government that whether "the physical characteristic yields incriminating information is *not* the dividing line between whether a compelled act comprises testimonial communication or not," and that the Supreme Court in *Doe* rejected the conflation of those two issues. *Id.* at 805. "That distinction—between whether an act is testimonial versus whether the act is incriminating—explains why physical characteristics, like fingerprints, blood samples, handwriting, and so on are not protected by the privilege even though they often are highly incriminating. . . . If the act does not *inherently* contain a communication from the person, then no testimony has been obtained from the person." *Id.*

The Magistrate Judge also did not acknowledge another recent published decision that undermined her reasoning: *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d 523 (D.D.C.

1 2018). There, the district court held that “the compelled use of the Subject’s biometric features” is not  
2 testimonial under the Fifth Amendment:

3           As other courts have recognized, there will be no revelation of the contents  
4 of the Subject’s mind with the procedure proposed by the government for  
5 collection of the Subject’s biometric features. Rather, “[t]he government  
6 chooses the finger to apply to the sensor, and thus obtains the physical  
characteristic—all without the need for the person to put any thought at all  
into the seizure.”

7 *Id.* at 535–36 (collecting cases) (quoting *In re Search Warrant Application for [Redacted Text]*, 279 F.  
8 Supp. 3d at 804). The district court went on to conclude that “the use of the fingerprint is much more  
9 like the government’s compelled use of other ‘physical characteristics’ of criminal suspects that courts  
10 have found non-testimonial even when they are used for investigatory purposes rather than solely for  
11 identification.” *Id.* at 536 (citations omitted). As the district court observed, “The ‘distinction which  
12 has emerged’ as a ‘helpful framework for analysis’ is that the Fifth Amendment ‘privilege is a bar  
13 against compelling communication or testimony, but that compulsion which makes a suspect or accused  
14 the source of real or physical evidence does not violate it.’” *Id.* (quoting *Schmerber*, 384 U.S. at 764)  
15 (internal quotation marks omitted). Again, the Magistrate Judge made no effort to grapple with this  
16 well-reasoned adverse authority.

17       Nor did the Magistrate Judge acknowledge adverse state-court authority, such as *Minnesota v.*  
18 *Diamond*, 905 N.W.2d 870, 876 (Minn.) (“[Defendant’s] act of providing a fingerprint to the police was  
19 not testimonial because the act did not reveal the contents of [his] mind.”), *cert. denied*, 138 S. Ct. 2003  
20 (2018). And while the Magistrate Judge did cite *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL  
21 10355635, at \*4 (Va. Cir. Ct. Oct. 28, 2014)—a case cited by the U.S. District Court for the District of  
22 Columbia in the decision discussed above—the Magistrate Judge ignored the Virginia court’s holding  
23 that law enforcement could use a subject’s fingerprint to unlock a phone, and that “[t]he fingerprint . . .  
24 does not require the witness to divulge anything through his mental processes.” The Magistrate Judge  
25 cited *Baust* only for the proposition that giving up a *passcode* is testimonial. See ECF No. 1 at 4.

26       Finally, the Magistrate Judge’s “functional equivalence” theory—under which the government  
27 may not use biometrics such as a face or fingerprint to unlock a device because biometrics are the  
28 functional equivalent of a passcode—also contravenes Supreme Court case law. A key to a safe is the

1 functional equivalent of a combination. Yet the Supreme Court, at least in dicta, has distinguished  
2 compelling the disclosure of a key from compelling the disclosure of a combination. *See Doe*, 487 U.S.  
3 at 210 n.9; *Hubbell*, 530 U.S. at 43; *In re Search of [Redacted] Washington, DC*, 317 F. Supp. 3d at  
4 535–36.

### 5 CONCLUSION

6 The Magistrate Judge’s order—issued without the benefit of any briefing—is contrary to law and  
7 should be reversed or vacated. The Magistrate Judge’s constitutional analysis is fundamentally flawed.  
8 And the order, if allowed to stand, will hinder the government’s ability to conduct lawful searches  
9 pursuant to valid warrants. For these reasons, the Court should overrule or vacate the order.

10 Dated: January 23, 2019

Respectfully submitted,

11 DAVID L. ANDERSON  
12 United States Attorney

13 /s/  
14 ROBERT S. LEACH  
15 JONAS LERMAN  
16 Assistant United States Attorneys  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 DAVID L. ANDERSON (CABN 149604)  
United States Attorney

2 HALLIE HOFFMAN (CABN 210020)  
3 Chief, Criminal Division

4 ROBERT S. LEACH (CABN 196191)  
JONAS LERMAN (CABN 274733)  
5 Assistant United States Attorneys

6 1301 Clay Street, Suite 340S  
Oakland, California 94612  
7 Telephone: (510) 637-3680  
FAX: (510) 637-3724  
8 robert.leach@usdoj.gov  
jonas.lerman@usdoj.gov

9 Attorneys for United States of America

10 UNITED STATES DISTRICT COURT  
11  
12 NORTHERN DISTRICT OF CALIFORNIA  
13 OAKLAND DIVISION

14 IN THE MATTER OF THE SEARCH OF A ) **CASE NO. 19-MJ-70053 JD**  
15 RESIDENCE IN OAKLAND, CALIFORNIA )  
16 ) **UNITED STATES' NOTICE OF**  
17 ) **SUPPLEMENTAL AUTHORITY**  
18 )

19 The United States writes to notify the Court of a pertinent recent decision from another court in  
20 this circuit.

21 Three days ago, Chief Judge David C. Nye of the District of Idaho decided *In the Matter of the*  
22 *Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, No. 19-MJ-10441-DCN, 2019  
23 WL 3401990 (D. Idaho July 26, 2019), vacating the order of a magistrate judge who had denied the  
24 government's search warrant application.

25 In that search warrant application, the government "sought permission to place a subject's finger  
26 on a cellphone to unlock the phone to conduct a forensic search." *Id.* at \*1. The magistrate judge  
27 denied the application. *Id.* Like Magistrate Judge Westmore here, the Idaho magistrate judge held "that  
28 the compelled pressing of the fingerprint to the cellphone sensor would violate the Fifth Amendment's



1 privilege against self-incrimination.” *Id.* at \*3. The magistrate judge “reasoned that compliance with a  
2 warrant authorizing an attempt by law enforcement to unlock the phone with the individual’s  
3 fingerprints inescapably requires a compelled testimonial communication because the individual would  
4 provide a ‘compulsory authentication of incriminating information’ and would ‘aid in the discovery,  
5 production, or authentication of incriminating evidence.’” *Id.* (citation omitted).

6 The government moved the district court to reverse or vacate the magistrate’s order. *Id.* at \*1.  
7 Chief Judge Nye granted the government’s motion.

8 First, Chief Judge Nye ruled that the matter was not moot—even though “any decision by the  
9 court in this case will have no impact on this case,” since too much time had passed for the government  
10 to unlock the cellphone in question with a fingerprint. *Id.* at \*2–\*3. “The prevalence of cellphones  
11 continues to rise and the Government’s applications for search warrants for biometric data likewise  
12 continues to rise. A search warrant must be processed within 48 hours of the Government’s seizure of a  
13 cellphone or the biometric data becomes meaningless.” *Id.* at \*3. Chief Judge Nye therefore concluded  
14 that “[t]his situation fits the ‘capable of repetition, yet evading review’ exception to the mootness  
15 doctrine,” and so the government’s “motion can be heard and decided despite the mootness of the issue  
16 due to this exceptional situation.” *Id.*

17 Turning to the merits, Chief Judge Nye held that the warrant would not violate the Fifth  
18 Amendment because biometric decryption involves no testimonial communication. *Id.* at \*3–\*7. After  
19 reviewing caselaw—and disagreeing with the magistrate’s decision here, *id.* at \*6—Chief Judge Nye  
20 concluded:

21 Where, as here, the Government agents will pick the fingers to be pressed  
22 on the Touch ID sensor, there is no need to engage the thought process of  
23 the subject at all in effectuating the seizure. The application of the  
24 fingerprint to the sensor is simply the seizure of a physical characteristic,  
25 and the fingerprint by itself does not communicate anything. It is less  
26 intrusive than a forced blood draw. Both can be done while the individual  
sleeps or is unconscious. Accordingly, the Court determines—in  
accordance with a majority of Courts that have weighed in on this issue—  
that the requested warrant would not violate the Fifth Amendment because  
it does not require the suspect to provide any testimonial evidence.

27 *Id.* at \*7 (footnotes omitted).

28 //

1 The decision is attached.

2 DATED: July 29, 2019

Respectfully submitted,

3  
4 DAVID L. ANDERSON  
United States Attorney

5  
6 /s/  
JONAS LERMAN  
7 ROBERT S. LEACH  
8 Assistant United States Attorneys  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28